



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
 FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
 PLAN DE ESTUDIOS DE LA LICENCIATURA EN INFORMÁTICA
 Sistema Escolarizado: Modalidad Presencial
 Programa de estudios de la asignatura



Informática forense

Clave 0592	Semestre 8°	Créditos 8	Campo de conocimiento: Informática	
			Eje de formación: Profesionalización	
Modalidad	Curso (X) Taller () Lab () Seminario () Otros ()		Tipo	T (X) P () T/P ()
Carácter	Obligatorio () Optativo (X) Obligatorio E () Optativo E ()		Horas	
Duración (Número de semanas)	16		Semana	Semestre
			Teóricas: 4	Teóricas: 64
			Prácticas: 0	Prácticas: 0
			Total 4	Total 64

Seriación

Ninguna ()

Obligatoria ()

Asignatura antecedente	
Asignatura subsecuente	
Indicativa (X)	
Asignatura antecedente	Seguridad informática
Asignatura subsecuente	Ninguna

Objetivo general:

Al finalizar el curso, el alumnado aplicará las técnicas para la obtención de información relevante que le permitan a las personas interesadas actuar en consecuencia.

Objetivos particulares:

Al finalizar el curso, el alumnado:

1. Obtendrá un panorama general de los campos en los que se aplica la informática forense.
2. Aplicará las técnicas para recuperar y autenticar la evidencia en los diferentes dispositivos de almacenamiento.
3. Aplicará las técnicas para mantener libre de contaminación la evidencia, así como la preservación de la fuente de ésta.
4. Distinguirá las técnicas para la obtención de información que revele el nivel de implicación de una persona en la comisión de un delito.
5. Hará con base en el análisis forense, el dictamen final de su investigación que permita a las autoridades actuar en consecuencia.

Índice temático			
Unidad	Tema	Horas Semestre	
		Teóricas	Prácticas
1	Introducción a la informática forense	6	0
2	Evidencia digital	10	0
3	Preservación del material informático	18	0
4	Análisis forense	16	0
5	Presentación del dictamen pericial	14	0
Total		64	

Estrategias didácticas

- Exposición audiovisual
- Exposición oral
- Ejercicios dentro de la clase
- Trabajos de investigación
- Prácticas de taller o laboratorio
- Lecturas obligatorias
- Desarrollos de proyecto
- Estudio de casos
- Uso de TI

Evaluación del aprendizaje

- Exámenes parciales
- Exámenes finales
- Trabajos escritos
- Tareas fuera del aula
- Participación en clase
- Proyecto de aplicación

Perfil profesiográfico del docente	
Título o grado	Licenciatura en Informática o equivalente, preferentemente con estudios de posgrado con orientación a las tecnologías de la información y las organizaciones.
Experiencia docente	Mínima deseable de 2 años impartiendo clases en nivel media superior y/o superior.
Otras características	<p>Experiencia Profesional mínima de 3 años en área de conocimiento. Experiencia en informática forense.</p> <p>Para profesoras/es de nuevo ingreso: Haber aprobado el “Curso Fundamental para profesores de Nuevo Ingreso (Didáctica Básica)” que imparte la Facultad de Contaduría y Administración, así como cubrir satisfactoriamente los requisitos impuestos por el departamento de selección y reclutamiento de la Facultad de Contaduría y Administración.</p> <p>Para profesoras/es que ya imparten clases en la Facultad: Haber participado recientemente en cursos de actualización docente y de actualización disciplinar con un mínimo de 20 horas.</p> <p>Compartir, respetar y fomentar los valores fundamentales que orientan a la Universidad Nacional Autónoma de México.</p>

Bibliografía básica
<ul style="list-style-type: none"> ◦ Bayuk, J., y Yoran, A. (2010). <i>Cyberforensics: understanding information security investigations</i>. U.S.A: Springer. ◦ Cano, M. J. (2013). <i>Inseguridad de la información: una visión estratégica</i>. Colombia: Alfaomega ◦ Doherty, E. P. (2013). <i>Digital forensics for handheld devices</i>. Boca Raton, Florida: CRC Press. ◦ Hurtado García, C. (2014). <i>Los aspectos más importantes de la ley federal de protección de datos personales en posesión de particulares</i>. México. ◦ Johnson, L. (2014). <i>Computer incident response and forensics team management: conducting a successful incident response</i>. E.U.: Syngress. ◦ Lázaro, F. (2013). <i>Informática forense: introducción</i>. Colombia: Ediciones de la U. ◦ Li, C. (2010). <i>Handbook of research on computational forensics, digital crime, and investigation: methods and solutions</i>. Hershey, E.U.: Information Science Reference. ◦ Meña, J. (2011). <i>Machine learning forensics for law enforcement, security, and intelligence</i>. E.U.: CRC Press. ◦ Pacio, G. (2015). <i>Data centers hoy - protección y administración de datos en la empresa</i>. México: Alfaomega. ◦ Piñar, J. L., Omelas, L., y Stoddart, J. (2013). <i>La protección de datos personales en México</i>. México: Tirant lo Blanch

Bibliografía complementaria
<ul style="list-style-type: none"> ◦ Arboledas, D. (2014). <i>BackTrack 5: hacking en redes inalámbricas</i>. México: Alfaomega ◦ Cross, M. (2014). <i>Social media security: leveraging social networking while mitigating risk</i>. E.U.: Syngress. ◦ García, J. P., Fernández, Y., Ochoa, Á., y Ramos, A. (2014). <i>Hacking y seguridad en Internet</i>. España: Ra-Ma. ◦ Gómez, Á. (2014). <i>Seguridad en equipos informáticos</i>. España: Starbook. ◦ Katz, M. (2013). <i>Redes y seguridad</i>. México: Alfaomega. ◦ Pearson, S., y Yee, G. (2013). <i>Privacy and security for cloud computing</i>. Reino Unido: Springer. ◦ Ramos, A., Barbero, C. A., González, J. M., Picouto, F., y Serrano, E. (2015). <i>Seguridad perimetral, monitorización y ataques en redes</i>. Colombia: Ra-Ma. ◦ Yang, K., y Jia, X. (2014). <i>Security for cloud storage systems</i>. E.U.: Springer.